U. S. DEPARTMENT OF ENERGY

HEADQUARTERS

MASTER INFORMATION SYSTEMS SECURITY PLAN

for Classified Personal Computers

October 1, 1999

Revision 1 (02/22/00)

Classified Information Systems Security Site Manager Approval:

/s/ Bonita Agee 10/01/99

Classified Information Systems Security Operations Manager Approval:

/s/ Jack Cowden 10/01/99

U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer
Office of the Associate CIO for Cyber Security
Operations Division

(THIS PAGE INTENTIONALLY LEFT BLANK)

Department of Energy Headquarters Master Information Systems Security Plan for Classified Personal Computers

INTRODUCTION

This plan implements the requirements of DOE O 471.2A, Information Security Program dated 3/27/97, and DOE M 471.2-2, Classified Information Systems Security Manual dated 8/3/99. Which augments the HQ Facilities Master Security Plan dated January 1995 with changes 1, 2, 3, 4, 5, 6, 7 and 8 dated 5/3/99 for the protection of classified information processed, stored, or produced on automated information systems (IS) of the Department of Energy (DOE) Headquarters (HQ). The plan also implements guidance specified in the memorandum titled “Personal Portable Computer (PPC)/Laptop/Personal Digital Assistant (PDA) restrictions” dated 7/21/99 written by, the Headquarters Classified Information System Security Operations Manager.

For the purpose of this security plan IS and System are synonymous and include all of the following - as single-user systems (used by only one person at a time) being used in a stand-alone mode such as personal computers, portable personal computers, personal digital assistants, dedicated word processors, and as remote terminals connected via Secure Telephone Unit-III (STU-III) Secure Data Devices (SDDs) to an accredited host computer, as terminals connected to STU-III Secure Voice/Data Set (SV/DS) equipment for limited, nonscheduled transmittal of data and as nodes (personal computers) connected by secure communications media to accredited networks.

Where the distinction between personal computer model types is necessary in this security plan, desktop and tower models are referred to as desktop computers and portable models are referred to as laptop computers. Personal digital assistants (PDA)s are considered the same as laptop computers, except where noted. Memory typewriters are not used at the HQ to process classified data, and are, therefore, omitted from this Master IS Security Plan. Should the need arise to process classified information on memory typewriters, the Classified IS Security Site Manager must first be contacted for guidance.

The Master IS Security Plan has been approved for general use; however, it alone does not fully meet the requirements for an approved security plan and cannot be used as the sole basis to gain accreditation to process classified information.

Individual IS operated under the authority of this plan will each be identified in one of the Attachment 5, Individual Security Plan, which details specific system characteristics not covered in one of the subsections of this plan. All of the requirements in the plan **must** be met. Any additions to or deviations from the requirements in this Master IS Security Plan will be documented in sections V and VI of Attachment 5.

Each Individual Security Plan must be separately approved by the Classified Information Systems Security Officer (ISSO) and forwarded to the Classified Information Systems Security Site Manager (ISSM) with certification that it meets the requirements of the Master IS Security Plan. The ISSM will review the Individual Security Plan, verify the ISSO's certification, and accredit the system under the authority delegated by the Classified Information Systems Security Operations Manager (ISOM).

All reorganizations which result in changes of users and/or ISSO responsibilities must immediately be brought to the attention of the ISSM so that resulting actions necessary to update the Individual Security Plans can be developed.

The Master IS Security Plan and Individual Security Plans specifically do not apply to mainframe host systems, local area network servers/controllers, connected disk-less user workstations or other multi-user IS. It does, however apply to individual user work stations (personal computers) connected as nodes to local area networks.

Classified Facsimile Devices and Digital Copiers are now covered by a separate master information system security plan as shown below.

The following items are available for viewing and/or downloading from the DOE Headquarters Computer Security Program Web Site at: **http://cio.doe.gov/compsec/**

- HQ DOE Master Information Systems Security Plan for Classified Personal Computers, with Attachments, dated 10/01/99, Rev 1 (2/22/00).
- Individual Attachments, dated 10/01/99, Rev 1 (2/22/00).
- The DOE HQ Master Information Systems Security Plan for Facsimile Devices and Digital Copiers, dated 10/01/99.

REFERENCES

DOE O 200.1, Information Management, dated 9/30/96.

DOE M 200.1-1, Telecommunications Security Manual, dated 3/15/97.

DOE N 205.3, Password Generation, Protection and Use, dated 11/23/99.

DOE G 205.3-1, Password Guide, dated 11/23/99.

DOE O 471.2A, Information Security Program, dated 3/27/97.

DOE M 471.2-1B, Classified Matter Protection and Control Manual, dated 1/6/99.

DOE M 471.2-2, Classified Information Systems Security Manual, dated 8/3/99.

DOE M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, dated 7/15/94 Change 1, dated 4/10/96.

Personal Computer Security Quick Reference Guide, dated 7/98 (revised 7/12/99).

Headquarters Security Officer's STU-III Procedural Guide.

DOE HQ Facilities Master Security Plan, dated January 1995 with changes 1, 2, 3, 4, 5, 6, 7 and 8 (Change 8, dated 5/3/99). **Available at http://nninfo.nn.doe.gov/**

NN-514.2 Memorandum, dated 2/26/96, Subject: Deviation from the Headquarters Master Automated IS Systems Security Plan for Automated Office Support Systems dated 2/26/96.

The DOE HQ Master Information System Security Plan for Facsimile Devices and Digital Copiers, dated 10/01/99.

DOE Statement of Generic Statement of Threat to Information Systems (2/97).

Memorandum titled “Personal Portable Computer (PPC)/Laptop/Personal Digital Assistant (PDA) restrictions” dated 7/21/99

Note: DOE Orders and Manuals are available at:

http://www.explorer.doe.gov:1776/htmls/directives.html

THIS PAGE INTENTIONALLY LEFT BLANK)

TABLE OF CONTENTS

(THIS PAGE INTENTIONALLY LEFT BLANK)

Department of Energy
Headquarters
Master IS Security Plan
for Classified Personal Computers

1. IDENTIFICATION AND LOCATION OF THE SYSTEM

1.1 Facility/Organization Name and Address

Headquarters
Germantown
United States Department of Energy
19901 Germantown Road
Germantown, Maryland 20874

Headquarters
Forrestal
United States Department of Energy
1000 Independence Avenue, S.W.
Washington, D.C. 20585

1.2 System Location

The specific location of each system is identified in the applicable Individual Security Plan (Attachment 5). The location specified for desktop computers is the room number of the limited/exclusion area where the desktop is installed. For laptop computers location is the room number of the limited/exclusion area(s) where the laptop computer will exclusively be used. System accreditation will be immediately revoked if a laptop computer is removed from its assigned location or when a property pass is issued for the laptop. The Accredited Portable Computer Validation Card (Attachment 7) will reflect the DOE Headquarters security area(s) in which the laptop will be used.

1.3 Accreditation Information

IS at the HQ are individually accredited to process classified information up to, and including, the highest classification level and most restrictive category identified in Paragraph VII-5 of the applicable Individual Security Plan (Attachment 5). **Only DOE owned computer equipment may be accredited to process classified information**. Accreditation of the system referred to in the

Individual Security Plan is effective upon completion of the signature of the ISSM in Paragraph VII-4. Information systems at DOE Headquarters are accredited for varying periods of time from 6 months to 36 months depending on certain conditions and criteria, including: type of hardware; processing location; level of classification of the information to be processed; etc. See Attachment 3, Accreditation/Re-accreditation Period Matrix for specific details.

1.4 Classified Information Sensitivity Level of Concern

Level of Concern	Qualifiers
High	All SCI All Special Access Programs (SAPs)/Special Access Required (SAR) All information protecting intelligence sources, methods, and analytical procedures All Single Integrated Operational Plan (SIOP) All Crypto SECRET RD (SIGMAs 1, 2, 14, 15) TOP SECRET
Medium	SECRET SECRET RD (All other SIGMAs)
Low	CONFIDENTIAL

Note: The DAA or the data custodian may determine that additional protection measures (beyond those required by the specific level of concern) are necessary to achieve an acceptable level of risk.

5. IS SECURITY ENVIRONMENT

5.1 Protection Level

A protection level of 1 (one) has been established for all systems (Desktop Computers and Laptop Computers) operating in a single-user/stand-alone capacity with no connection to another computer. This is based on the fact that only one U/SO with the appropriate clearance level and required "need-to-know" is allowed access to an individual system at any given time in accordance with DOE O 471.2A and DOE M 471.2-2.

When connected to another computer (Host, LAN or another desktop computer) (connection with a host or LAN is identified in Section III of the Individual Security Plan), the protection level of the system changes from 1 (one) to 2 (two). This is because the U/SO of one connected system may not have a "need-to-know" for all information contained on the host or other connected system.

Any system (Desktop Computer or Laptop Computer) with a protection index greater than 3 (three) must be accredited under a separate security plan.

5.2 Methods Used

The methods used to meet the above requirements will be described in Paragraphs 6 through 10 of this Plan. **All security measures identified in this plan <u>must</u> be implemented. All deviations <u>must</u> be identified in Section V of Attachment 5. Any security measures implemented in addition to those mentioned in this plan <u>must</u> be identified in Section V of Attachment 5.**

5.3 Individual System Description

5.3.1 All Personal Computers

Individual Security Plans describe each IS and identify the sensitivity level of concern, and the highest classification level and most restricted category of the information to be processed. IS equipment is included in each HQ organization's property accounting inventory. A risk review was conducted on the methods of assigning, distributing, installing, and supporting IS software and hardware at the HQ. This risk review has shown that sufficient controls have been placed on each element of the procurement, storage, installation planning, installation, maintenance, and software support to minimize the risk of unauthorized targeting of specific hardware and software packages to classified areas. Each Individual Security Plan will, however, list the following information:

a. System Identification Number, as assigned by the ISSM.

b. Location

# Building, Room (see Paragraph 1.3)

# Responsible organization, official

c. Hardware

# CPU Manufacturer

# CPU Model

# DOE Property Tag Number on CPU

d. Operating System Software, Security Related Software and Communications Software

# Developer

# Product Name

# Version Number

In addition to the information required above, all Personal Computers (Desktop and Laptop Computers) used to process classified information must comply with the requirements of DOE N 205.3, Password Generation, Protection and Use, dated 11/23/99. It is strongly recommended that Microsoft Windows NT version 4.0 or later is used as the operating system. Additionally, the operating system settings for Services/Devices, Passwords and Auditing must be configured as shown on Attachment 2. The Software Technician or ISSO is required to initial each item on Attachment 2 to indicate that the configuration complies with these requirements. The ISSM support personnel will initial each item to indicate that they have checked and verified the configuration.

Attachment 2 is submitted with the Individual Personal Computer Security Plan (Attachment 5) and the Security Review Checklist for Personal Computer

Certification (Attachment 4) to apply for approval to process classified information.

5.3.2 Additional Requirements for Portable Personal Computers (Laptop Computers)

Because of the risks associated with processing classified information on laptop computers DOE management will justify the risk and explain why a laptop computer is necessary versus a typical desktop computer. A completed Statement of Security Risk (Attachment 8) must be included with the attachments above and will serve as the risk justification for the laptop.

5.4 System Security Testing

As part of the accreditation process, the system is reviewed for compliance with this Master IS Security Plan and its associated Individual Security Plan. Attachment 4 presents a brief security compliance checklist that is used as an aid in the compliance review process. The accrediting official has determined that compliance reviews adequately test the security implemented for the system being accredited.

5.5 Modification Controls

The U/SO is responsible for bringing all planned system modifications to the attention of the ISSO at the earliest opportunity. All modifications planned for accredited IS will be discussed with the ISSO prior to implementation. The ISSO will analyze the proposed modification to determine the expected impact on security caused by the changes and, if applicable, gain any approval required of the TEMPEST Coordinator, SO-332/GTN, or other security official. In addition, the Individual Security Plan must be updated to reflect the modification, and forwarded with appropriate attachments for certification and re-accreditation (See also, Paragraph 17 for applicability.)

5.6 Periods Processing

The term "periods processing" denotes the method of operation used at DOE HQ to allow accredited IS to operate securely within sequential processing sessions of distinctly differing levels of information sensitivity (from **NON-SENSITIVE UNCLASSIFIED** up to, and including the highest processing level (based on classification and category) of information the system is accredited to process).

Periods processing provides the capability to either:

a. Sequentially, have more than one user on a single-user accredited IS with different levels of information or need-to-know;

b. Sequentially, use an accredited IS at more than one processing level and/or;

c. Transmit or receive different levels of information or need-to-know.

Only accredited desktop computers and laptop computers with removable hard disks can perform periods processing. Accredited desktop and laptop computers with permanently fixed hard disk drives may <u>not</u> perform periods processing. <u>All computers, desktops, laptops and personal digital assistants containing internal fixed hard disk drives must be accredited for use at the highest classification level and conspicuously marked with the appropriate classification level and category markings.</u>

Accredited desktop computers and laptop computers employed in periods processing shall have at least two separate sets of media, one for unclassified processing, and one for classified processing (each distinct level of classification i.e., Top Secret stand-alone, Special Access Program stand-alone, Secret Restricted Data stand-alone, Classified LAN, etc.) including operating systems, utilities, and applications software.

Where two or more U/SOs share a desktop computer or laptop computer <u>and</u> a single classified hard disk drive, the Windows NT operating system version 4.0 or later is required because it provides access control for need-to-know separation and audit trail capability. If the U/SO's do not have the same need-to-know authorization the use of the Windows NT operating system is mandatory.

Accredited systems are sanitized in accordance with Paragraph 10.5 before making the transition from a processing session with higher classification/category to a processing session of lower classification/category. They are also sanitized between processing sessions when all U/SOs who have had access to the system since the last sanitization process have differing need-to-know restrictions than those U/SOs who are to be given subsequent access to the system.

Accredited desktop computers and laptop computers with removable hard disks may be used to process data in a strictly unclassified environment only after the system has been sanitized to the unclassified level in accordance with procedures stated in Paragraph 10.5 of this Plan. During periods of processing in an unclassified mode, all data processed will be handled in accordance with the policy stated in DOE O 200.1, Information Management, with the exception that all input and output magnetic media must be individually marked "UNCLASSIFIED" in accordance with procedures detailed in Paragraph 10.4 of this Plan. All other security controls (Physical, Administrative, Hardware/Software, Telecommunications, and Personnel) must comply with this Plan.

5.6.1 Accredited Desktop Computers Connected to Networks

Accredited desktop computers (approved to process classified information) may be connected to networks (unclassified LAN and/or accredited classified LAN) only when **all** of the conditions specified in this paragraph are met:

The desktop computer must not be configured with fixed hard disk drives. The desktop computer must be configured to use removable hard disk drives. The user must have at a minimum two separate removable hard disk drives (one classified and one unclassified). The hard drives will be marked and stored as required in Paragraph 10.4 of this plan. The desktop computer must be configured to boot (load the operating system) from the removable hard drives. Communication software (e.g., DOECOMM) may only be installed on the classified hard disk drive when the desktop computer is approved to communicate with other classified computer systems via SDD.

An approved mechanical switching device, e.g., A/B Switch Box, must be used as an interface and positive disconnect between the desktop computer and the LAN connection(s). See Paragraph 5.6.3 for a list of approved mechanical switch boxes. See Paragraph 5.6.4 for A/B switch marking requirements.

5.6.1.1 Accredited Desktop Computer Connected to an Unclassified LAN

In addition to the requirements in Paragraph 5.6.1 above, an accredited desktop computer connected to an unclassified LAN may not have any LAN operating system software (i.e., lsl.com, ipx.odi, etc.) installed on the classified hard disk drive. The A/B switch box will be configured in a manner that connects the unclassified LAN cable to the "A" connector port. The "B" port is isolated because it will not be connected.

5.6.1.2 Accredited Desktop Computer Connected to an Unclassified LAN and an Accredited Classified LAN

In addition to the requirements specified in Paragraph 5.6.1, an accredited desktop computer connected to both an unclassified LAN and an accredited classified LAN must meet the following requirements: The hard drive signature packets (established by the LAN configuration file during boot-up) will be set at a value of "3" for the classified hard drive and a value of "0" for the unclassified hard drive. The A/B switch box will be configured in a manner that connects the unclassified LAN cable to the "A" connector port, and the classified LAN cable to the "B" port. Further, passwords must be unique between unclassified networks and classified networks. See DOE G 205.3-1, Password Guide for more information on passwords.

5.6.2 Sanitization Procedures for Switching from Classified LAN to Unclassified LAN

Before processing UNCLASSIFIED information, the user must perform the following:

! The user must log off of the classified LAN, the classified hard disk drive must be removed, perform all required sanitization routines as specified in Paragraph 10.5 of this plan and turn off the power for the entire system, including all peripheral devices for at least 1 minute.

! The A/B selector switch must be repositioned to the "A" position.

! The unclassified removable hard disk drive will be placed in the hard drive receptacle (in the computer) and the computer will be powered on.

! The U/SO may now process unclassified information.

5.6.3 Approved Mechanical Switch Boxes

The following mechanical switch boxes are currently approved for use with classified desktop computers: SW045A (DB15s connectors), QVSCA284-2 (RJ45 connectors, used for Macintosh computers), and SW046A-FFMFF (DB15s connectors) 5 position.

5.6.4 A/B Switch and Transceiver Marking Requirements

The A/B selector switch will be marked with an "Approved for Classified" sticker on the top or side where it can be easily seen. Additionally the switch will be marked to indicate "A" as "Unclassified" and "B" as "Classified". Plastic self sticking marking labels may be used for this purpose. A green label embossed with a “U” for unclassified, and a lavender label embossed with a ”C” for classified. The transceiver for the classified LAN must be marked to indicate that it is classified. SF-709, lavender “Classified” labels should be used for this purpose. The transceiver for the unclassified LAN must be marked unclassified. SF-710 “Unclassified” label should be used.

5.7 Maintenance Swap Controls

Hardware and software systems occasionally suffer failure due to old age, manufacturing defects, and other - normally unforeseen - reasons. When failures occur, maintenance personnel normally replace the affected hardware or software items with like (same manufacturer, model, and version numbers) items in good repair, and the affected items are turned in for repair or replacement and returned to the supply stock. If like items in good repair are not available as "loaners" or replacements, then compatible items are sometimes used. If the item being replaced is the CPU, and the replacement is identical, the system does not have to be re-accredited, however the individual security plan (Attachment 5) must be updated to show the DOE property number of the replacement CPU and a copy of the updated Attachment 5 submitted to the ISSM with a note that the CPU has been replaced. If the affected item cannot be replaced with a like item, the U/SO must notify the ISSO, who must then gain re-accreditation of the "new" or "changed" system (Paragraph 17 may also be applicable).

5.8 Acquisition Specification

DOE and DOE Contractor organizations shall ensure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition of hardware, software, or related services to be utilized in a classified environment. The ISSO will be included in the planning process for any new hardware or software procurement or developments that apply to classified in the DOE HQ environment especially for the acquisition of computer hardware because many cannot be accredited due to inherent technical vulnerabilities. (See Paragraph 4.1, above.)

(THIS PAGE INTENTIONALLY LEFT BLANK)

8. TELECOMMUNICATIONS SECURITY

Each communications link used to support an accredited IS is protected commensurate with the level of classification and category of the information for which the system is accredited. The protection features of each link are implemented in accordance with DOE M 200.1-1, Telecommunications Security Manual.

The only dial-up, point-to-point communications authorized for use with classified information among accredited desktop computers, laptop computers, and other automated information resources (e.g., host computers) are those provided by National Security Agency-approved encryption devices (e.g., NES and the STU-III family of devices).

8.1 Commercial Non-encrypting Modems

The use of any internal or external modem, FAX/modem, or dial-up capable data path unit to process unclassified information with an accredited desktop computer represents a very high risk and is therefore prohibited except under the following circumstances. Internal modem/Fax cards/network/PCMCIA boards are prohibited in laptop computers. These devices must be removed or disabled.

If the U/SO of an accredited desktop computer needs unclassified communications capability to perform their official duties and that service is either not available, is impractical, or otherwise cannot be accomplished through an unclassified LAN then a Statement of Security Risk (Attachment 8) must be executed. Additionally, Section V (Deviations from DOE HQ Master IS Security Plan) of the Individual Personal Computer Security Plan (Attachment 5) must be completed and the system must be re-accredited.

Once accredited, desktop computers operating under the provisions above must adhere to the following procedures:

! The modem and/or FAX/modem must only be used to process **unclassified** information;

! Data communications software may only be installed on the unclassified removable hard disk drive, unless the system has an authorized connection to a STU-III device or an accredited classified LAN;

! The modem or FAX/modem must be connected to the telephone line through an approved mechanical switching device (A/B switch) that provides a positive disconnect from the phone line when processing in the classified mode. The unclassified telephone line must be connected to the "A" side of the switch and nothing connected to the "B" side of the switch;

- When processing **unclassified** information, all classified media must be removed from the desktop computer and stored in an approved security container. The entire desktop computer configuration must be sanitized by turning off power prior to turning the A/B switch to the position for unclassified processing, the unclassified removable hard disk drive inserted into the desktop computer and the system re-booted.

8.2 STU-III Secure Voice/Data Set (SV/DS)

These procedures outline the minimum requirements for use by an IS of a STU-III SV/DS (the variety of models supporting both voice and data) as an encryption device for the limited, nonscheduled, point-to-point transmission of ad hoc data. Use of a STU-III SV/DS for the scheduled transmission of classified information is not covered by this plan. In such cases, the requirements of DOE M 471.2-2, relating to the accreditation of networks, must be met.

Section III of Attachment 5 will be appropriately annotated and the system accredited by the ISSM prior to use. An "Approved for Classified" label must be affixed to the STU-III SV/DS prior to any classified data transmission.

The person initiating a secure data transmission is responsible for verifying that the recipient and the facility where the computer will be connecting is authorized to receive and properly store the transmitted classified information. This is accomplished through the Safeguards and Security Information Management System (SSIMS).

- To initiate secure data transmission, a valid Cryptographic Ignition Key (CIK) must be locked into the STU-III SV/DS and confirmation of the secure mode must be received and indicated. (Note: CIK/STU-III must encrypt or be equal to the level of classification of the hard disk drive.)

- STU-III must not go secure at the unclassified level.

- Properly cleared personnel with the proper "need-to-know" must be present at both terminals, during the entire period of interconnection. This ensures by visual verification that the proper classification level and identification information of the STU-III SV/DS display matches the classification of the data being transmitted and the recipient's need-to-know.

! It is the responsibility of both sender and receiver to ensure that no data is transmitted that is of a higher classification level or more restrictive category than their highest common clearance/access level.

! Removable hard disks in the IS must be the same level of classification and category as the data to be processed. To prevent a higher classification of data being sent than is authorized, visual inspection of the data before transmission by the sender is mandatory.

8.3 STU-III Secure Data Device (SDD) Model 1900/1910

These procedures outline the minimum requirements for using SDDs as the primary means for protecting point-to-point communications between accredited IS and an accredited host computer or in point to point operation with other devices external or internal to the HQ.

Installation, operation, maintenance, and removal of each SDD terminal will be in accordance with procedures presented in the STU-III Procedural Guide.

To initiate secure data transmission, a valid Cryptographic-Ignition Key must be properly inserted into the SDD and confirmation of the secure mode must be received and indicated before communications can proceed.

The U/SO may not leave the SDD unattended while it is in the secure mode of operation.

When not in use, the crypto-ignition key must be removed from the SDD and either carried on the user or stored in a repository authorized for the classification level of the SDD.

8.4 Emission Security

The ISSO must contact the DOE Headquarters TEMPEST Coordinator before |
installing computer equipment (new installs) to schedule a pre-installation site |
survey to ensure that the site is suitable for accredited system placement. Aperiodic checks are also performed by the ISSO and the ISSM to ensure continued compliance.

DOE Red/Black separation requires a minimum of: Six (6) inches of separation between Classified IS (<u>the entire system, including peripheral devices</u>) and <u>any part of an</u> unclassified IS (<u>entire system, including peripheral devices</u>); A minimum of two (2) inches of separation between classified and unclassified data lines.

In the situation where a classified desktop computer shares a peripheral device (such as a printer) and unclassified data lines and equipment with communications capabilities; Six (6) inches of separation between classified IS and telephones; and six (6) inches of separation between STU-III devices and classified and unclassified IS.

In addition to the separation requirements above, all classified data lines must be marked with red tape at the point of connection to the classified IS and at intervals that allow for easy recognition of those lines. Reference DOE M 200.1-1, Telecommunications Security Manual, Chapter 8, Transmission Security Protection Measures, dated 3/15/97, for specific details of separation requirements.

In the situation where a classified desktop computer shares a peripheral device (such as a printer) with a unclassified desktop computer, both desktop computers must be separated from the shared device and each other by at least 6 inches.

The separation requirements specified above do not apply to IS currently operating in an area that is covered under a TEMPEST Plan. Separation requirements for these systems are specified in their applicable TEMPEST Plan, and maintained by the Headquarters TEMPEST Coordinator, SO-332. Consultation with the TEMPEST Coordinator should be effected for those systems planned for these areas.

8.5 Wireless Communications

8.5.1 Wireless - Infrared (IR) Ports

The use of wireless communications (infrared) ports found on most laptop computers to interface with printers and other peripheral devices is strictly forbidden on accredited IS. These ports must be removed or disabled on all accredited computers and peripherals by covering the infrared (IR) window with black electrical tape and a numbered security seal or physically removing the infrared transmitter. The DOE Headquarters TEMPEST Coordinator will be responsible for making sure that all accredited Information Systems (IS) are in compliance with infrared port requirements while conducting the TEMPEST threat assessment.

8.5.2 Wireless - Radio Frequency (RF) Transmissions

Use of RF devices to transmit/receive sensitive or classified information is prohibited without NSA approved encryption device techniques. A TEMPEST special review must be conducted before an NSA approved encryption device can be used for RF transmission/reception of sensitive or classified information.

8.6 Remote Diagnostic Services

Remote diagnostic services are not permitted on accredited systems.

(THIS PAGE INTENTIONALLY LEFT BLANK)

10. ADMINISTRATIVE SECURITY

The following procedures have been established to ensure that all IS within HQ facilities have adequate administrative controls to restrict access to the appropriate U/SOs and to ensure the protection of classified IS assets.

10.1 Configuration Management

Configuration management procedures are used to ensure that development and changes to an IS take place in an identifiable and controlled manner.

The following four specific aspects of configuration management are used to provide assurance that modifications in the environment of the IS do not adversely affect the security of that system.

10.1.1 IS Configuration Identification

Configuration identification employs the identification of system components and documentation that supports security control procedures. In the Master IS Security Plan, requirements stipulate the necessary controls that will be used. Attachment 5, Individual Security Plan, provides the necessary support documentation. The following criteria is either in the Master IS Security Plan or will be identified in the Attachment 5, thereby establishing a system baseline to be used as a reference.

# Security control procedures, e.g., Personnel, Physical, Telecommunications, Software, Administrative.

# Modification control procedures.

# System-specific design documentation.

# Major Equipment Component Identification, Attachment 5.

# Equipment Configuration, Attachment 5.

# ISSO Certification date, Attachment 5.

# ISSM Accreditation date, Attachment 5.

10.1.2 IS Configuration Control

The task of configuration control is performed by subjecting system components and documentation to a review and approval process within the computer security organization. Configuration control is implemented by the Modification Controls, Paragraph 5.5. Modification controls identify the procedures used to evaluate, coordinate, and submit for approval requests for IS modifications.

10.1.3 IS Configuration Status Accounting

Status accounting is possible through both manual and online systems. The U/SO and ISSO account for the requirements defined in Paragraph 10.1.1 by means of the documentation required by this plan. The ISSM monitors the accreditation process and maintains accreditation files.

10.1.4 IS Configuration Auditing

Configuration auditing is accomplished via the review processes embodied in the Classified IS Security Program life cycle. Initially, the ISSO conducts an assurance review before recommending the system for certification. The ISSO also has the authority to exercise security oversight, at any time, IS within his/her responsibility to ensure that all control procedures identified in the Master IS Security Plan are used. Oversight of security control procedures is provided by the ISSM for the initial certification review and through periodic program compliance reviews by the ISOM. This continual auditing program assures that criteria stated in IS configuration identification are met.

10.2 Access Controls

Physical access control procedures are identified in Paragraph 7, Physical Security.

Microsoft Windows NT Operating System version 4.0 provides user identification and password for gaining access to the personal computer. The password used must comply with DOE N 205.3, Password Generation, Protection and Use, dated 11/23/99.

Laptop computers may only be used in limited/exclusion area shown on the Portable Personal Computer Validation Card, however they cannot be left unattended. When unattended, laptop computers must have the removable classified hard disks removed and stored in an approved security container, and the laptop computer must be sanitized by not only turning off the power switch, but the battery must also be removed and then the laptop placed in a security container.

Because laptop computers are not permanently installed, special care must be exercised when processing classified information. The following precautions must be taken:

- **!** Orient the computer where the screen and any printed material cannot be viewed by uncleared individuals, or post a "Classified Processing Do Not Enter" sign on the door to the room and close it.

- **!** Maintain proper separation from other electronic devices, telephones, and electrical equipment.

10.3 Installation Control Procedures

Control is applied at various checkpoints prior to the installation of an IS earmarked for classified processing. IS equipment received at DOE from the manufacturers is immediately controlled. Those items of equipment to be used for classified processing are selected at random from the store of existing stocks immediately prior to installation. This practice precludes the equipment from being targeted specifically for a classified installation until the last possible moment before the installation process.

10.4 Media Security

Access to IS storage media (i.e., magnetic disks or tapes, compact discs, paper, or printer ribbons) containing classified data will be restricted to individuals possessing the appropriate DOE clearance and approved need-to-know.

10.4.1 Marking of Removable Magnetic Media

10.4.1.1 Marking During Classified Sessions

The following marking and handling requirements do not apply to unclassified compact discs used in systems with verified read only CD drives. The marking and handling requirements do apply to diskettes containing software programs.

Prior to beginning a classified processing session on an accredited IS, all removable magnetic media and recordable CD(s) to be used during the session will be appropriately labeled for protection. Standard Form SF 709 ("CLASSIFIED" label) is no longer used to mark media and any storage medium currently labeled with SF 709 must be immediately reviewed and marked with the appropriate classification level and category. The appropriate classification label will be placed on diskettes (appropriate means the highest level and most restrictive category of information on the system's hard disk). Example shown at Attachment 6, Labeling Diskettes) the classification and category of data stored on the magnetic media may be identified on the first line of Standard Form (SF) 711, Data Descriptor Label (optional), or if SF-711 is not used, the category must be entered on the classification label. All classified 3 ½ inch diskettes may have SF 711 or equivalent placed in the center of the diskette label area with the appropriate classification label directly below (the excess is folded around the edge).

Removable hard disks will be labeled in the same manner as 3 ½ inch diskettes, on the disk casing and the container. Diskette folders and removable hard disk containers will be marked at the top and bottom, front and back, with the appropriate classification of data stored on the enclosed magnetic media. Most restrictive category markings will be placed in the lower left corner of the folder. Only properly labeled removable hard disks and diskettes are used to store or process classified data files. If a label is placed on the disk or folder to identify the individual documents contained on the disk, the appropriate portion marking designator will be placed parenthetically after the title of the document it governs.

The marking and handling requirements for removable magnetic media do apply to systems with recordable CD drives.

All Classified Compact Disc (CD) must be physically marked on both sides with the appropriate classification and category. These markings are placed on the hub of the CD, which is a narrow blank space adjacent to the center hole. See illustration in Attachment 6. One technique is to use a silk screening method that permanently marks the disk, another option is to use a classification stamp with permanent indelible ink that won't rub off.

<u>Warning: Do not put any classification stickers or other markings on the recording surface portion of the compact disc.</u>

Also, certain types of ink may cause damage to the surface of a CD. Users may want to test mark a blank CD before using an untried marking device on a CD containing information.

10.4.1.2 Document Marking Responsibilities

Users are responsible for properly marking classified electronic files (documents) transmitted or shared outside the user’s exclusive domain (the user's computer). Specifically, users are responsible for including all of the classification markings which appear on paper copies of documents, when classified documents (files) are in electronic form, including text within a database, spread sheet document, html, ascii text file, etc. The markings required include: Paragraph (portion) markings in the body of documents; classification level and category (if RD/FRD) markings at the top and bottom (header and footer) of each page, or at the beginning and end of the actual text on each page if header and footer markings are impractical or not available with the software used; subject line portion markings (regardless of category), name of the classifier and downgrading instructions, etc. (**NOTE**: Portion marking of text paragraphs is not required for documents/files containing RD/FRD; however, it is a sound security practice and is recommended.)

Examples of electronic files that must be marked include (but are not limited to): word processing, database, spread sheet, html, etc., documents; e-mail and/or attachments to e-mail; files that are shared in a peer-to-peer network (two or more desktop computers directly connected to each other); files that are posted to a classified network server for access by other than the originator; electronic files that are hand transmitted (physically handing the file to another person).

When e-mail messages include classified attachments, the e-mail message must contain a warning that the attachment is classified and specify the classification level and category (if RD or FRD) of the attachment, even though the e-mail message itself may not be classified.

Further, users who receive classified files created by another individual (internal or external to DOE) or whenever a classified file is printed or retransmitted are responsible for ensuring that the files (documents) are properly reviewed and/or marked by a derivative classifier/declassify, even though the document appears to be properly marked. This procedure will ensure that all classified documents are properly marked and no extra marking(s) have been added. If a user receives a classified document without the required markings, they must immediately notify the sender and request proper markings or accept the responsibility of properly marking the document before it is transmitted further or shared with another user. For more detailed information see the DOE HQ Facilities Master Security Plan.

10.4.1.3 Marking During Unclassified Sessions

Prior to being inserted into a sanitized, accredited IS during unclassified processing sessions, unclassified magnetic media will be labeled with SF 710

("UNCLASSIFIED" label). Mark recordable compact disc with a stamp or by hand on the hub as shown at Attachment 6. In addition, unclassified magnetic media known to contain sensitive information will be appropriately marked (I.e., OUO, UCNI, etc).

10.4.2 Marking of Fixed Magnetic Media

Desktop computers with fixed internal hard disk drives (Must be permanently located in a vault approved for the open storage of classified information) will be marked externally on the front of the system and internally on the hard drive casing the highest classification level and most restrictive category of data for which the system is accredited to process. Laptop computers with fixed internal hard disk drives may NOT be used to process classified information.

10.4.3 Storage Containers (Disk Holders)

Disk file folders or boxes, including those for compact disc will be marked in accordance with Paragraph 10.4.1, above, similar to files or folders containing classified information.

10.4.4 Personal Computer Monitors

During classified processing sessions, colored classification marking signs or DOE/DP-0018/1, Department of Energy Computer/Terminal Sensitive Data Warning Signs (sometimes referred to as a security flip-chart or tent sign) identifying the highest classification level and most restrictive category of information the IS is accredited to process will be prominently displayed.

10.4.5 Printouts

Specific guidance for reviewing, handling, storing and marking can be found in Chapter XI, Paragraphs 2 through 6 of the DOE HQ Facilities Master Security Plan.

10.4.6 Printer Ribbons

10.4.6.1 Dot Matrix Printer Ribbons

Multiple-strike printer ribbons used in dot matrix printers during classified processing are exempted from security labeling. Multiple-strike dot matrix printer ribbons may remain in the printer (do not have to be stored in a safe) at all times, as long as the printer remains in a limited area within the Germantown or Forrestal buildings of the HQ.

Single-strike ribbons used in dot matrix printers during classified processing are not exempted from security labeling--they must be labeled with the highest classification and most restrictive category of the data they are used to process.

Single-strike (e.g., carbon film) ribbons must be removed from the printer and stored in a safe when not in use or when the system is unattended or being used in an unclassified mode.

All dot matrix printer ribbons must, however, be destroyed as classified in the manner referenced in Paragraph 10.4.13, below.

10.4.6.2 All Other (Non-Dot Matrix) Printer Ribbons

Non-dot matrix printer ribbons used in classified processing sessions will be marked with the highest classification level and most restrictive category of information for which the IS is accredited to process. Non-dot matrix printer ribbons used during unclassified processing sessions (on sanitized IS that have been accredited for classified processing) will be marked with "UNCLASSIFIED" or "SENSITIVE UNCLASSIFIED," as the case may be.

10.4.7 Toner Cartridges

Toner cartridges may be left in laser printers without being marked with a classification label as long as the printer is in proper working order and has not malfunctioned during a printing operation, i.e. paper jam, etc., see Paragraph 10.5.3. for information on printer malfunctions. Also see Paragraph 10.5.3 for information on depleted toner cartridges.

10.4.8 Color Printer - Color Transfer Rolls

Some color printers use a color transfer roll in place of a ribbon or toner cartridge.   Once used the information that has been printed can be read on the roll. For this reason separate rolls must be used during classified and unclassified operations. The roll used for classified information must be marked and protected as specified for single strike (carbon film) ribbons (see Paragraph 10.4.6.1, above). When the classified roll is depleted and replaced it must be destroyed appropriately (see Paragraph 10.4.13, below).

10.4.9 Media Storage

All classified removable media, when not being used by the system (i.e., diskette/removable hard disk, CD(s), ribbons, hard copy reports, etc.), will be stored in a security container that is approved for the highest classification level and most restrictive category of data stored on the media.

10.4.10 Classified Software Protection

Media containing the operating and software systems used for classified processing sessions will be labeled and protected as appropriate for the highest level of classification and most restrictive category of information for which the IS is accredited to process. When the accredited IS is used for periods processing (for alternating classified and unclassified sessions), separate software systems must be maintained on separate media (removable hard drive, diskette, etc.); a classified version for use during classified sessions and an unclassified version for use during unclassified sessions.

10.4.11 Magnetic Media Sanitization Procedures

Sanitization refers to the elimination of classified information from (declassification of) magnetic media to permit the reuse of the media at a lower classification level or to permit the release to uncleared personnel or personnel who do not possess the proper information access authorizations.

There is currently no acceptable method for sanitizing classified magnetic media. Magnetic media that is unusable or no longer needed must be destroyed using the destruction procedures cited in Paragraph 10.4.13. Magnetic media should be "cleared" before being released to the destruction process. Clearing procedures follow in the next Paragraph.

10.4.12 Magnetic Media Clearing Procedures

"Clearing" magnetic media refers to a procedure by which classified information recorded on the media is removed, but the totality of declassification is lacking. Clearing is a procedure used when the magnetic media will continue to be safe-guarded within the controlled environment. Magnetic media will be cleared by overwriting the media a minimum of one time with any one character. Verification of the overwrite process may be accomplished by random reread of the overwritten information to determine that only the overwrite character can be recovered.

Cleared magnetic media may be reused or released for destruction; however, it will be marked and controlled at the level of the highest classification of data ever recorded.

The programs "CLRDSK.EXE," "CLRDSKC.EXE," and "CLRDISK.COM," previously used to clear magnetic media are no longer approved for use at DOE Headquarters.

The approved method to accomplish magnetic media clearing for systems using

Windows 3.11 operating system now uses Norton utilities for DOS (version 5.0 or higher) "WIPEINFO". For systems using Windows NT the preferred program is BCWIPE (**use by government organizations requires purchase of program**). These utility programs offer much more flexibility than the CLRDSK programs. Options are available that allow either the entire disk to be cleared, specific files on the disk, the unused portions of disks, or the slack area of a disk. Another option is "Wipe Methods". There are two choices. FAST WIPE and GOVERNMENT WIPE. FAST WIPE satisfies the minimum DOE HQ requirements. Government wipe provides additional assurance by writing 0s (zeros) followed by 1s (ones) 3 times, then writing the character with the decimal value 246 one time. For more information on the WIPEINFO or BCWIPE utilities consult your technical support personnel, or the computer security support team 903-2106 in Germantown or 586-5346 at the Forrestal building.

10.4.13 Destruction Procedures

Specific destruction procedures can be found in Chapter XI of the DOE Headquarters Facilities Master Security Plan.

10.4.14 Document (or Media) Accountability

The definition for "documents" includes "IS input and contents of equipment and/or media, including memory, punch cards, tapes, diskettes, removable hard disk drives, CD(s), and visual displays."

Magnetic media which is used in a sanitized, accredited computer when it is operating in the unclassified mode (the removable hard disk drive marked Unclassified is in the system) does not have to be placed in an accountability system.

Removable magnetic media will be appropriately labeled as described in Paragraph 10.4.1, above. The space marked "Control:" on the optional SF 711, Data Descriptor Label, will contain the accountability control number for the diskette, if applicable. If SF 711 is not used, the control number will be written on the Standard Form classification label. Once magnetic media is appropriately marked with the appropriate classification label it will be entered into the accountable document inventory file, if applicable, maintained by the ISSO or classified document custodian.

Accountable documents/media that are to be destroyed in accordance with procedures stated in Paragraph 10.4.13, will be annotated on DOE F 5635.9, "Record of Destruction."

10.5 System Sanitization

The accredited IS including all peripheral devices must be sanitized:

# Before being left unattended; (see Paragraph 4, Chapter XI of the DOE Headquarters Facilities Master Security Plan.)

# During periods processing:

" When ramping down from a session of higher level classification/category to a session of lower level classification/category.

" Before being used by another U/SO who doesn't possess the same access authorization and need-to-know.

" Before being repaired or sent off-site for repair by uncleared hardware technicians.

10.5.1 All IS

To sanitize the system, all media will be removed and stored in accordance with classified media storing specifications. System memory (to include the printer buffer and the buffers of any other peripheral devices) will be sanitized or purged of classified information (This is accomplished by turning off the power for the entire system including all connected peripheral devices and battery backup (if present on anything but clock-function chips or other printed circuit boards) for at least one minute). The system must then be re-booted with a separate copy of the software system that has been reserved for use during unclassified processing sessions only.

10.5.2 Laptop Computers

In addition to turning off external power (see 10.5.1 above), laptop computers also must have the battery or power pack removed in order to sanitize memory.

10.5.3 Laser Printer Toner Cartridges

Laser printer toner cartridges **no longer need to be sanitized** by printing 3 pages of random characters as long as the last print process was successfully completed. In the case of a paper jam, power failure during printing, etc., reprinting the document successfully will satisfy the need to clear or sanitize the toner cartridge.

Once sanitized, the laser printer toner cartridge may be released to unclassified channels for replenishment.

10.5.4 Color Printer - Color Transfer Rolls

To sanitize color printers that use the color transfer rolls, in addition to turning off the power to the printer, the transfer roll must be removed, marked with the proper security classification level, and stored in an approved security container.

10.6 Host Computer Access Controls

U/SOs that require access to LANs or other hosts computers must comply with the security plan for those systems and must follow the application procedures for those computer resources. IS connected to a host computer must be identified and authenticated through the use of userids and passwords. Security on the host computer is highly dependent on the proper protection of the passwords used to access them. Password management is the responsibility of the ISSO. Password protection is the responsibility of the U/SO. Procedures for protecting passwords can be found in the security plan for the specific system for which the U/SO has access.

10.7 Property Removal Authorization

A properly completed and approved DOE Property Pass must be presented to the security guard before exiting a HQ complex building with any Government/DOE piece of IS equipment, diskettes, magnetic cartridges, or removable hard drive cartridges, unless specifically exempted from the requirement by written authority. Classified magnetic media can only be removed from the HQ complex as outlined in Chapter XI, of the DOE HQ Facilities Master Security Plan.

10.7.1 Removal of Accredited Laptop Computers

See Paragraph 7.3.

10.7.2 Removal for Repair

Before removing an accredited desktop computer, laptop computer, or peripheral device from the room where it is installed for off-site repair the fixed hard disk or removable hard disk must be removed and stored in an approved security container and all "Approved for Classified" stickers or other markings that indicate use to process classified information must be removed.

10.7.3 Decommissioning Desktop Computers and Laptop Computers

When an accredited desktop computer or laptop computer is no longer going to be used for processing classified information, there are several actions that must take place to ensure that all classified information has been cleared from the system and that all markings that indicate that the desktop computer/laptop computer was previously used to process classified information have been removed from the hardware. The following paragraphs identify all of the steps required to transition a system to the unclassified environment.

10.7.3.1 Clearing Hard Disk

Fixed and removable hard disks used with a workstation that is being decommissioned must be cleared by overwriting the entire disk with any one character. The software program used to perform the overwrite should report disk sectors successfully overwritten and bad sectors that cannot be overwritten. If there are sectors of the disk that cannot be overwritten and a software program cannot be found that will overwrite the bad sectors, the disk will have to be destroyed. The ISSO must review the results of the overwrite procedure and verify that the overwrite was successful. Once cleared, the disk drive must be labeled with the highest level of the classified information the disk previously contained. <u>The disk may now be re-used only for classified processing by another user in another classified workstation</u>. If the disk is damaged and cannot be cleared by overwriting, it must be destroyed. Specific destruction procedures can be found in Chapter XI of the DOE Headquarters Facilities Master Security Plan.

10.7.3.2 Removing Fixed or Removable Hard Disk

Once the hard disk has been cleared and marked as specified in 10.7.3.1 above, it must be removed from the desktop computer and stored in an approved security container until needed. After removing the hard disk (ISSO must verify removal of hard disk and memory devices), remove all “Approved for Classified” and/or classification stickers from the desktop computer cabinet and peripheral devices. Once all markings that indicate that the desktop computer has previously been used to process classified information have been removed and the hard disk has been removed, the desktop computer and peripheral devices may be disposed of through normal channels, or used in the unclassified environment.

10.7.3.3 Reporting Decommissioning to the ISSM

When a desktop computer/laptop computer is decommissioned the ISSO must complete the top portion of an Individual Personal Computer Security Plan, Attachment 5. Enter the System ID (HQ number) assigned to the desktop computer by the ISSM when the desktop computer was accredited. Enter a “D” in the space for decommissioning. Enter the effective date for the decommissioning and sign in the space provided. The completed attachment is then submitted to the ISSM.

10.8 System Contaminations

If the unclassified hard disk of a desktop computer or laptop computer becomes accidentally contaminated by classified information, stop all processing, immediately log off shared system (e.g., Mainframe, Local Area Network), turn off the power to the desktop computer/laptop computer, protect the system and media and immediately contact the Hotline at 903-2500 and your ISSO. Continue to protect the system until someone from the hotline arrives. Laptop computers can be placed in an approved security container until assistance arrives. See Paragraph 14, Incident Reporting, below for more requirements. Incident details may be sensitive or classified. Callers should only give their name, phone number and room number.

10.9 Analog or Digital Audio/Video Recording Capabilities of IS

Microphones/Video Cameras in computers used in areas designated for classified or sensitive unclassified discussion must be removed or disabled. Any exceptions to this policy that are needed to support extenuating conditions, (e.g., physically challenged) and then only with the employment of additional safeguards (e.g., soundproofing, etc.), will only be granted after the user first obtains a deviation in accordance with Paragraph 5, Chapter III of the DOE HQ Facilities Master Security Plan and then approved by the ISSM prior to enabling.

(THIS PAGE INTENTIONALLY LEFT BLANK)

11. WASTE, FRAUD, AND ABUSE

11.1 Definition and Reporting

Waste, fraud, and abuse incidents in which computers and/or their peripherals are involved are to be reported and addressed through the perpetrator’s direct line of management. These types of incidents are a violation of the Code of Federal Regulations and the Federal Employees Code of Ethics.

The definitions of waste, fraud and abuse are as follows:

Waste - Misuse of computer time (i.e., games, private use, use of unauthorized software), or resources, whether intentional or not.

Fraud - Illegal activities, including misrepresentation, personal gain, copyright violations.

Abuse - Intentional alteration or destruction of software, hardware, or information.

11.2 Recognition of Copyrights and Licensing Agreements

User non-compliance with software copyright and licensing agreements is a violation of Federal Law. HQ Elements are to monitor compliance as part of their information management activities. Incidents are to be reported and addressed within the perpetrator’s direct line of management.

11.3 Warning Banners

All computer systems at DOE Headquarters must display (electronically or written/printed page posted on the monitor) the warning banner shown on the next page during the start-up process. The computer must continue to display the banner until closed by the user.

Warning Banner

NOTICE TO USERS
This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site,
Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties.

By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree

12. RISK IDENTIFICATION

A qualitative risk identification has been performed for IS at the Germantown and Forrestal facilities. This identification is general in nature because it encompasses all IS within these facilities. The level of protection provided each IS is based on the U/SOs knowledge of the security procedures detailed in this plan.

12.1 Risks

The following table (continued on next page) identifies some specific risks to accredited IS, their probability of occurrence rating (i.e., Low, Moderate, High), the impact of an occurrence, and implemented countermeasures.

RISKS	PROB	IMPACT	COUNTERMEASURES
Fire	Low	High	Fire extinguishers, some areas protected by fire suppression systems.
Power Disturbances	Low	Low	Systems protected by surge protection devices.
Power Outages	High	Low	U/SOs are required to backup data on a regular basis.
Water Damage	Low	Low	Construction of building and placement of IS negates water damage.
Malicious Authorized U/SOs	Low	Low	All U/SOs processing classified have security clearances and have been trained in the protection of classified information and the systems that process classified information.
Covert Action	Low	Low	Building guards, visitor controls, and use of approved safes for document, removable magnetic media, and ribbon storage. Limited Security Areas with electronic and combination locks control access. Hardware and software procurement, installation, and support cannot be targeted to accredited IS.

RISKS	PROB	IMPACT	COUNTERMEASURES
Casual Visitors	Low	Low	Posted signs for classified processing, room divider around accredited systems in some rooms, visitor controls, magnetic media removed during non-use periods, 3-way combination locks and limited security areas control access.
Emanation	Low	Low	Use of TEMPEST-protected or other DOE-approved low-emanation equipment.
Natural Hazards	Low	Low	Inherently secure/safe building.
System Abuse	Low	Low	Monitoring by supervisor and the ISSO. Personnel security briefings.
Physical Damage to Portable (Laptop) Computers	High	Low	Portability of laptop computers make them vulnerable to damage from being dropped. Padded carrying cases and removable hard disks reduce the risks substantially.
Theft of Portable (Laptop) Computers	Moderate	High	This threat is reduced by storing laptop computers and removable magnetic media in approved security containers, and user vigilance.

12.2 Asset Identification

All items of IS equipment and operating systems software are considered low value assets. Each equipment and operating system asset will be identified in the Individual Security Plan. The information files (to include such files as data, query routines, or application software) processed on these systems may be of higher value; therefore, U/SOs have been cautioned to protect their information investment by performing regular backups and storing them at a prudently safe distance from their primary working copy.

12.3 Summary of Qualitative Risk Identification

The qualitative Risk identification chart, Paragraph 12.1, depicts the risk management technique used to identify and counter known and potential risks. Based on the analyses of these risks and the fact that all classified processing is performed within DOE Security Areas, the protection mechanisms implemented for these areas are deemed sufficient for the low value assets covered by this plan. Except for IS located in vaults approved for open storage of classified information, see Paragraph 3, Chapter IX of the DOE HQ Facilities Master Security Plan for specific guidance on the control of all classified media. All classified media must be controlled (if necessary) by document-accountability procedures. The protection mechanisms implemented within the Security Areas for the protection of documents have been evaluated by the ISSM and deemed sufficient for the protection of the information processed.

(THIS PAGE INTENTIONALLY LEFT BLANK)

13. TRAINING

13.1 ISSOs

All ISSOs are required to attend the ISSO Training Class provided by the ISSM. As a minimum, the ISSOs will provide the following instructional material to each U/SO.

# Master IS Security Plan. The ISSO and U/SO must retain a copy of the currently approved Master IS Security Plan for IS at their respective systems. These copies may be maintained in an electronic format (as a data file), in lieu of maintaining a printed copy. Electronic copies of the Plan and its Attachments (blank forms) may be downloaded from the DOE Headquarters Computer Security Program Web Site at: http://cio.doe.gov/compsec/.

# Personal Computer Security Quick Reference Guide.

13.2 U/SOs

All classified IS U/SOs are responsible for reading the documents cited above.

Each responsible U/SO will read the Master IS Security Plan for IS (and the security plans for any system or network to which their accredited work station is connected) annually. The responsible U/SO will, also annually, sign Attachment 1, Code of Conduct, accepting responsibility for the security of their assigned IS.

13.3 Computer Security-Trained Escort.

To qualify as a computer security-trained escort, the candidate must have received all the training listed in the previous Paragraph for U/SOs and must be technically competent to escort and observe repair technicians. Questions concerning technical competence will be determined by the ISSO.

(THIS PAGE INTENTIONALLY LEFT BLANK)

14. INCIDENT REPORTING

In order to thwart deliberate and/or malicious acts (i.e., equipment tampering, Trojan horses, virus programs) directed at IS, all personnel utilizing DOE IS resources will observe the following procedures for reporting any perceived attacks. Also, any occurrence of a security infraction will be reported using the procedures below. These procedures will permit each U/SO to properly report potentially damaging incidents. By initiating the following actions in a timely manner, U/SOs may assist in controlling and limiting the damage that may be caused by an incident.

14.1 Incident Recognition by U/SO

Upon noticing or suspecting unusual or uncharacteristic performance from your system, suspend processing on the affected system. Attempts to determine the cause through use of the system may distort or destroy any evidence investigators might need to identify and/or correct the situation.

14.2 Notification Procedures

U/SOs are to immediately notify, through secure means (e.g., face-to-face, encrypted voice), the responsible ISSO (and/or Alternate ISSO) of the affected system concerning the possibility of a successful threat occurrence. This will allow the ISSO to immediately begin a preliminary inquiry and notify other potential targets, thereby limiting further potential damage. If the ISSO or Alternate is not readily available, call the ISSM. Minor incidents associated with the use of IS (generally those whose adverse impact can be contained within the authority and responsibility of the ISSO) need not be reported to the ISSM, but are to be documented, investigated, and resolved by the ISSO.

Incidents whose scope and adverse impact extend beyond the authority and responsibility of the ISSO (e.g., LAN or mainframe connectivity is involved) are to be communicated to the ISSM as soon as practical. The intent is to coordinate efforts to limit the potential damage which could be incurred.

14.3 Documentation and Review

After incident notification, the U/SO will annotate the following information, if known, for use by security personnel.

a. Time of Occurrence

b. Source of Problem (e.g., imported software, diskette/hard disk drive, etc.)

c. Nature of the Incident - explain what happened prior to and during the occurrence.

d. The U/SO should review DOE Headquarters Facilities Master Security Plan Chapter XVI, Security Incidents/Infractions/Violations Program for more guidance.

15. CONTINGENCY PLANNING

In general, IS equipment assets are low cost, easily replaceable items. However, contingency planning is addressed for all systems that process classified information, as follows.

15.1 Critical Resources

It is the responsibility of the U/SO to identify any hardware configuration or software system that is considered critical for the successful completion of the DOE mission. If a system is designated as critical, backup procedures and matching system configurations must be identified in writing to ensure continuity of operations. Additional procedures, specific to the critical system, will be identified in the Individual Security Plan for the critical system. These procedures must be tested annually. All IS identified as critical will be backed up by the U/SO once a week, at a minimum, and the backup media will be stored at an alternate location that is reasonably distant from the primary processing and information storage site.

15.2 Non-Critical Resources

All non-critical systems will be backed up by the U/SO on a regular basis to assure a continuity of the operations that support the conduct of the DOE mission.

(THIS PAGE INTENTIONALLY LEFT BLANK)

16. ESCORT PROCEDURES

Visitors (cleared, but without a need-to-know, or uncleared) to office areas where accredited IS are present must be escorted in accordance with DOE Headquarters Facilities Master Security Plan and may not be permitted physical access to accredited IS or to view classified information. In addition, escorts for visitors who are going to have access to the inside of an accredited computer (uncleared repair technician) must be computer security-trained in accordance with Paragraph 13.3 of this plan.

(THIS PAGE INTENTIONALLY LEFT BLANK)

17. INTERIM OPERATING PROCEDURES

The following procedures govern the operations of accredited desktop computers in the interim periods during updates or changes to their environment. These procedures do not apply to laptop computers or personal digital assistants. The environment of an accredited IS encompasses those items of hardware and software listed in Attachment 5; the location of the IS; the assigned U/SO; and, the approved security controls in place at the time of the current accreditation.

Interim re-accreditation is granted for a period of 10 work days only for those systems previously accredited and only under the following conditions:

! U/SO Changes,

! Hardware replacement with similar equipment,

! Software changes, or

! System relocations within an existing HQ security area.

Interim accreditation begins when the change is effected (e.g., hardware has been reinstalled at the new location).

If not re-accredited in these 10 work days, the system accreditation will be considered revoked and will only be authorized to process unclassified information.

<u>NOTE</u>: These are administrative changes. Changes that affect the security of the system must be immediately coordinated with the ISSM.

(THIS PAGE INTENTIONALLY LEFT BLANK)

USER/SECURITY OFFICER CODE OF CONDUCT

(TO BE COMPLETED AND SIGNED BY THE U/SO ANNUALLY)

U/SO's Initials

1. ____ I have read the Master IS Security Plan and am familiar with its contents. I have also read the security plans for all accredited systems and networks that my work station is connected to and I am familiar with their contents. Additionally, I have read the Personal Computer Security Quick Reference Guide.

2. ____ I am aware of my responsibility for knowing what constitutes a security infraction and the procedures for responding to an infraction.

3. ____ I am aware of my responsibility for reporting any incidents of data intrusion or other security-related events to the Classified Information Systems Security Officer (ISSO) in accordance with current DOE and local policy.

4. ____ I am aware that, when the system is to be left unattended, accredited systems must be sanitized, and that classified computer media, such as removable hard drives, diskettes, compact disc (CD ROM), cassettes, single-strike printer ribbons, and printed output must be locked in a DOE approved security container.

5. ____ I am aware that individual passwords must be unique, must comply with the guidelines specified in DOE N 205.3, are intended only for the assigned user, and may not be shared with anyone else. I am responsible for protecting passwords and records of passwords used with classified IS at the highest level and most restrictive category approved for the IS.

6. ____ I am aware that I must establish/determine an individuals need-to-know prior to sharing, providing access to, or forwarding any sensitive unclassified or classified information.

7. ____ I am aware that users of classified systems are to prevent (to the extent possible) unauthorized persons from entering the work area during classified processing and that the IS must be positioned so that it cannot be viewed from outside the processing area (i.e., in view from open doors or uncovered windows). I am further aware that users must logoff of classified IS and remove and properly store all media prior to leaving the system unattended.

8. ____ I am aware that all data should be backed up periodically to preclude the need for extensive reconstruction of files following a system failure or emergency. I am also aware that, ideally, these files should be stored in a separate remote location.

9. ____ I am aware that classified media and printed output and their covers or containers must bear appropriate classification markings that indicate the highest level of data contained therein. I am further aware of my responsibility to follow Document (or Media) Accountability Procedures located in Paragraph 10.4.14 of the Master IS Security Plan .

10. ____ I am aware that removable hard drives, diskettes, CD ROM, cassettes, tapes, toner cartridges, printed output, and printer ribbons used for classified processing must be sanitized, declassified, and/or destroyed according to the policies, practices, and procedures listed in Paragraph 10.4 of the Master IS Security Plan.

11. ____ I am aware of and will comply with the procedures specified in the Master IS Security Plan Paragraph 5.6.2 regarding system sanitization and proper transition between LAN connections and stand-alone processing.

12. ____ I am aware of my responsibility to continually improve security. Through my daily interaction with a system, I am able to detect weaknesses and vulnerabilities within the system. I will make a conscientious effort to express ideas on enhancing security to the designated ISSO.

13. ____ I am aware that, as a U/SO of Department of Energy systems, I must ensure that the equipment is used only for job related processing and that all other uses are prohibited.

14. ____ I am aware that electronic equipment, antennas, etc., may not be placed in the immediate proximity of the classified IS without being listed and approved by the ISSM in the Individual IS Security Plan. I am also aware that any modifications to the IS, either in addition to or deletion of hardware or software, may not be performed without the prior approval of the ISSO.

15. _____ I am aware that only DOE-authorized software may be used on an accredited IS. I will abide by any licensing agreements applicable and am aware that any software copyright and licensing infringements are violations of Federal law.

* In addition to the statements above, <u>Only</u> users of Laptop Computers must attest to statements 16 through 27.

16. _____ I am aware that I must contact ISSO when password lockout occurs.

17. _____ I am aware that I must only use a Laptop Computer to process classified information in the limited/exclusion area(s) specified on the Individual Security Plan (Attachment 5) for my system. I am also aware that removal of the system from its assigned location or issuance of a property pass for my system will result in immediate revocation of the accreditation of the system.

18. _____ I am aware that processing classified information at sites other than Headquarters requires additional approval, and I am responsible for securing local Information Security Site Manager (ISSM) approval to process classified information.

19. _____ I am aware that prior approval of the SSO must be obtained by the responsible user before introducing the Laptop Computer into a Sensitive Compartmented Information Facility.

20. _____ I am aware that I must turn off all electrical power sources for at least 1 minute including physical removal of the battery in order to sanitize the Laptop Computer.

21. _____ I am aware that Laptop Computers are highly vulnerable to theft and must be given appropriate protection when in my possession, especially in public places.

22. _____ I am aware that I am responsible for notifying the ISSO of any maintenance, hardware, software or configuration change(s) prior to any such modifications.

23. _____ I am aware that the classified removable hard disk and any classified diskettes must be transported by DOE approved methods.

24. _____ I am aware that I am responsible for security of all equipment and information processed on the Laptop Computer.

25. _____ I am aware that classified information must be stored in accordance with DOE Orders.

26. _____ I am aware that I am restricted to processing classified information (S/RD) at approved DOE facilities. Processing of classified information (S/RD) outside of approved DOE facilities must be approved in writing.

27. _____ I am aware that I must have a copy of and comply with the Headquarters Master Information Systems Security Plan, Systems Accreditation Documentation, Individual Security Plan and the Accredited Portable Personal Computer Validation Card. Copies of this documentation must be maintained with the computer at all times.

I have read the above statements and understand my responsibilities for protecting classified systems and information as indicated by my initials. I am aware that I am required to review, initial, and resign this form annually no later than the anniversary date as indicated next to my signature below.

U/SO: ______________________________ ______________________________ ____/____/____

Printed Name *Signature* *Date*

Instructions

The purpose of this form is to provide a documented means of insuring that each U/SO is aware of his/her responsibilities for processing classified information on an IS.

This form contains a series of statements, for which the U/SO will initial each to indicate that he/she understands and acknowledges his/her responsibilities. This will be done annually (not later than 1 year from the date signed on the previous form) by each U/SO to provide a refresher to the U/SO of his/her responsibilities. After the U/SO has completed this form (all the statements are initialed) and the ISSO is confident that the U/SO understands his/her responsibilities, then the ISSO may allow the U/SO to perform classified processing on an accredited IS. This form is not required to be submitted with the accreditation/re-accreditation package to the ISSM, but will be reviewed by the ISSM representative when a site or compliance review is held. The ISSO will retain the original of this form until replaced by the next annual form completion and provide a copy of same to the U/SO for reference purposes.

(THIS PAGE INTENTIONALLY LEFT BLANK)

PORTABLE PERSONAL COMPUTER
CONFIGURATION DESCRIPTION SUPPLEMENT

1. Purpose

This Laptop Computer configuration description supplements the Individual Security Plan (Attachment 5) for the portable personal computer identified as HQ-______.

2. Configuration Description

This Laptop Computer will use Windows NT 4.0 as the operating system. The tables below indicate the settings/set-up for certain features/devices. See reverse side of this form for additional configuration requirements.

The technician responsible for setting up the Laptop Computer for classified use will initial in the spaces provided to indicate that the Laptop Computer has been configured as required. The ISSM support personnel will verify each setting with their initials in the appropriate space.

SERVICE/DEVICE	REQUIRED SETTING	TECHNICIAN INITIALS	SECURITY INITIALS
Infrared Port	*Disabled*		
Internal Modem	*Disabled*		
Microphone	*Disabled*		
Password Features	*Enabled*		
Auditing Features	*Enabled*		

3. Password Features

FEATURES	TECHNICIAN INITIALS	SECURITY INITIALS
Password is eight (8) characters (see next page for required format), with lock feature turned on.		
Password expiration period is 180 days.		
User is permitted to change NT account password.		
Lock out threshold for unsuccessful log-on attempts has been set at 3.		
User lock out duration is 60 minutes. *(See reverse side of this form)*		

4. Auditing Features

FEATURES	SETTINGS		TECHNICIAN INITIALS	SECURITY INITIALS
Log on and off		*Failure*		
File and object access *(See reverse side of this form)*	*Success*			
Use of User rights		*Failure*		
User and group management	*Success*	*Failure*		
Security policy changes	*Success*	*Failure*		
Process tracking *(See reverse side of this form)*	*Success*			

Portable Personal Computer
Configuration Description Supplement

Explanation of Configuration requirements:

1. <u>User Password</u> Strong passwords enabled, i.e. must comply with the following guidelines:

a. Passwords must be at least eight non-blank characters.

b. Passwords must be a combination (mixture) of upper case alphabetic characters (A - Z), lower case alphabetic characters (a - z), numeric characters (0 - 9) and at east one special character (!, @, #, %, etc.) In the first seven positions.

c. Password must be a non-numeric character in the first and last position.

d. Null characters are not permitted (i.e. space)

e. Password must not be the User ID.

f. Password for users classified system must <u>not</u> be the same as password for users unclassified system.

2. <u>User lock out duration</u> should be set at 60 minutes. If the user is locked out, he/she has the option of waiting 60 minutes before attempting to log in again or having the ISSO reset the lock out before the 60 minute lock out expires.

3. The <u>audit event log</u> should be set up to overwrite as needed to avoid unnecessary user lock outs if the log should become too large.

4. When setting up users in User Management, disable "Guest". Set up an account named ISSO with Administration rights. Password for this account is to be the given to the ISSO.
To ensure user lock out can be reset quickly in emergency situations it is recommended that the ISSO put the password in a sealed envelope marked with the appropriate classification and category and store the sealed envelope in a security container.

5. <u>File and Object Access auditing</u> refers to the Windows NT operating system, not necessarily users files. Auditing of user files greatly increases the amount of data stored in the audit logs.

6. <u>Process Tracking</u> as specified by the ISSO.

For a complete description of password requirements see DOE N 205.3 Password Generation, Protection and Use, dated 11/23/99.

Attachment 4

SECURITY REVIEW CHECKLIST
FOR
PERSONAL COMPUTER CERTIFICATION

SYSTEM ID: HQ-________(ISSM WILL ASSIGN)DATE:_____/_____/_____ ORGANIZATION:_____________________

LOCATION: BUILDING:_________________________ ROOM NUMBER:_________________

	PRINTED NAME	SIGNATURE	DATE
U/SO			
ISSO			
REVIEWED BY			
ISSM STAFF			

NUMBER OF "APPROVED FOR CLASSIFIED" STICKERS REQUIRED:_________

QUESTIONNAIRE	YES	NO
1. IS THE CERTIFICATION DOCUMENTATION COMPLETE AND ACCURATE?		
2. IS THE SYSTEM LOCATED (OR STORED AND USED IF A LAPTOP) IN A LIMITED AREA (WITHIN SECURITY ISLANDS OR IN OFFICES LOCKED WITH DOE-APPROVED LOCK?		
3. ARE WARNING SIGNS AVAILABLE FOR WORK STATIONS WHERE THE MONITOR CAN BE SEEN BY UNCLEARED PEOPLE?		
4. ARE DOE/DP-00181/1, DOE COMPUTER/TERMINAL SENSITIVE DATA WARNING SIGNS (CLASSIFICATION LEVEL FLIP CHART SIGNS) AVAILABLE FOR THE SYSTEM?		
5. IS THE SYSTEM CONFIGURED TO DISPLAY THE WARNING BANNER (SHOWN ON PAGE 11-2 OF THE MASTER IS SECURITY PLAN FOR CLASSIFIED PERSONAL COMPUTERS DURING THE START-UP PROCESS OR IS A PAPER COPY OF THE WARNING BANNER POSTED ON OR NEAR THE SYSTEM?		
6. IS THE U/SO AWARE OF THE CLASSIFIED DOCUMENT/MEDIA MARKING LABELING PROCEDURES AND IS THERE EVIDENCE OF ADEQUATE SUPPLIES OF LABELING STOCK? IF THIS IS A RE-ACCREDITATION REVIEW, IS THERE EVIDENCE OF PREVIOUS COMPLIANCE WITH MARKING/LABELING PROCEDURES?		
7. IS THE U/SO AWARE OF THE PROPER PROCEDURES FOR COMPLYING WITH CLASSIFIED DOCUMENT/MEDIA ACCOUNTABILITY REQUIREMENTS? IF THIS IS A RE-ACCREDITATION REVIEW, IS THERE EVIDENCE THAT ALL THE MEDIA (CLASSIFIED/UNCLASSIFIED) IS PROPERLY MARKED WITH THE LEVEL/CATEGORY?		
8. IF THE COMPACT DISC DRIVE HAS THE CAPABILITY TO RECORD, IS THE U/SO AWARE OF THE MARKING POLICIES FOR CD'S?		
9. IS RED/BLACK SEPARATION IN COMPLIANCE, OR IF SYSTEM IS A LAPTOP IS THE U/SO AWARE OF AND COMPLY WITH RED/BLACK SEPARATION REQUIREMENTS WHEN USING SYSTEM?		
10. ARE ALL CLASSIFIED DATA LINES MARKED WITH RED TAPE AT THE POINT OF CONNECTION TO THE CLASSIFIED EQUIPMENT AND AT INTERVALS THAT ALLOW EASY RECOGNITION OF THOSE LINES? (OR, IF NOT, HAS NOTIFICATION BEEN MADE TO THE HQ TEMPEST COORDINATOR TO INSPECT AND MARK THE LINES?)?		
11. IS THE U/SO KNOWLEDGEABLE OF BACK-UP PROCEDURES, AND, IF THIS IS A RE-ACCREDITATION REVIEW AND APPLICABLE, ARE SYSTEMS DATA AND PROGRAMS ADEQUATELY BACKED-UP?		
12. IS THE SYSTEM MAINTAINED AND SUPPORTED BY SO-30 (OR, IF SYSTEM IS NOT MAINTAINED AND SUPPORTED BY SO-30, HAVE MAINTENANCE PROCEDURES BEEN APPROVED BY THE ISSM AND INCLUDED IN THE INDIVIDUAL PERSONAL COMPUTER SECURITY PLAN?)?		
13. IF THE SYSTEM CONTAINS AN INTERNAL OR EXTERNAL NON-ENCRYPTING MODEM OR FAX/MODEM TO PROCESS UNCLASSIFIED INFORMATION DOES THE U/SO HAVE A SIGNED STATEMENT OF SECURITY RISK?		
14. IF THE SYSTEM IS EQUIPPED WITH AN INFRARED PORT HAS IT BEEN DISABLED?		
15. IF THE SYSTEM IS NOT LOCATED IN A VAULT THAT IS APPROVED FOR OPEN STORAGE OF CLASSIFIED MATTER, HAS THE INTERNAL FIXED HARD DISK BEEN REMOVED AND REPLACED WITH A REMOVABLE HARD DISK?		

QUESTIONNAIRE (CONTINUED)	YES	NO
16. HAS THE HARD DISK DRIVE, FIXED OR REMOVABLE, BEEN MARKED (HIGHEST CLASSIFICATION AND MOST RESRRICTIVE CATEGORY OF THE INFORMATION STORED) INTERNALLY ON THE DRIVE HOUSING AND EXTERNALLY ON THE REMOVABLE CARTRIDGE COVER?		
17. IF THE SYSTEM IS EQUIPPED WITH A MICROPHONE, HAS IT BEEN REMOVED OR OTHERWISE DISABLED?		
18. IS THE SYSTEM CONNECTED TO A CLASSIFIED AND/OR UNCLASSIFIED LAN, AND IF SO IS THE CONNECTION THROUGH AN APPROVED MECHANICAL SWITCH (A = UNCLASSIFIED AND B= CLASSIFIED)?		
19. IF THE SYSTEM IS NOT CONNECTED TO A CLASSIFIED LAN AND/OR AUTHORIZED FOR TRANSMITTING CLASSIFIED INFORMATION USING A STU-III TYPE DEVICE, HAS ALL COMMUNICATION SOFTWARE, INCLUDING ALL MAIL COMMUNICATION SOFTWARE BEEN ELIMINATED FROM THE CLASSIFIED REMOVABLE HARD DRIVE?		
20 IS ACCESS TO THE SYSTEM PROTECTED BY A PASSWORD THAT COMPLIES WITH DOE N 205.3, PASSWORD GENERATION, PROTECTION AND USE?		
NOTE: THE FOLLOWING QUESTIONS MAY NOT BE APPLICABLE TO THE SYSTEM BEING REVIEWED. IF NON-APPLICABLE, ENTER N/A IN THE "YES" COLUMN.		
21. IS THE U/SO AWARE OF THE LASER PRINTER TONER CARTRIDGE SANITIZATION REQUIREMENTS AND PROCEDURES (I.E., PRINTING 3 PAGES NO LONGER REQUIRED.)?		
22. IF APPLICABLE, IS THE U/SO AWARE THAT THE COLOR TRANSFER ROLLS USED IN SOME COLOR PRINTERS MUST BE REMOVED, MARKED AS CLASSIFIED AND STORED IN AN APPROVED SECURITY CONTAINER WHEN THOSE PRINTERS ARE UNATTENDED?		
23. IF APPLICABLE, AND IF THIS IS AN INITIAL CERTIFICATION REVIEW, IS THE U/SO AWARE OF PROCEDURES FOR USING A STU-III SV/DS OR SDD FOR DATA COMMUNICATIONS? IF APPLICABLE, AND THIS IS A RE-ACCREDITATION REVIEW, IS THERE EVIDENCE OF COMPLIANCE WITH THE PROCEDURES?		
24. IF THE SYSTEM USES FIXED MAGNETIC STORAGE MEDIA (DESKTOP COMPUTERS ONLY), OR IF THE SYSTEM IS LOCATED, STORED AND/OR USED IN AN APPROVED VAULT, IS THERE EVIDENCE OF CERTIFICATION FROM THE HEADQUARTERS OPERATIONS DIVISION (NN-514) DOCUMENTING THEIR APPROVAL FOR OPEN STORAGE OF CLASSIFIED INFORMATION?		
25. IF THIS IS A RE-ACCREDITATION REVIEW, AND IF THEY ARE USED ON THIS SYSTEM, ARE NON-DOT MATRIX PRINTER RIBBONS MARKED WITH THE HIGHEST CLASSIFICATION LEVEL AND MOST RESTRICTIVE CATEGORY OF INFORMATION THAT IS PRINTED?		

SECURITY REVIEW CHECKLIST FOR PERSONAL COMPUTER CERTIFICATION

INSTRUCTIONS

THIS FORM IS PROVIDED TO AID THE U/SO IN DOCUMENTING HIS OR HER ASSURANCE THAT THE IS BEING REVIEWED IS CERTIFIABLE AS MEETING ALL THE APPLICABLE IS SECURITY REQUIREMENTS NECESSARY TO PROCESS CLASSIFIED INFORMATION IN A SECURE ENVIRONMENT.

THE CHECKLIST CONTAINS A SERIES OF QUESTIONS, FOR WHICH YES OR NO ANSWERS WILL SUFFICE. ALL OF THE QUESTIONS APPLY, AND EACH MUST BE ANSWERED IN THE AFFIRMATIVE BEFORE THE SECURITY OF THE IS CAN BE CERTIFIED BY THE ISSO TO THE ISSM.

WHEN ALL OF THE QUESTIONS HAVE BEEN ANSWERED IN THE AFFIRMATIVE, AND THE U/SO AND THE ISSO ARE SATISFIED THAT ADEQUATE PROTECTION HAS BEEN PROVIDED FOR THE SECURITY OF THE SYSTEM, THE SIGNED AND DATED FORM MUST BE FORWARDED IN A PACKAGE, ALONG WITH THE INDIVIDUAL PERSONAL COMPUTER SECURITY PLAN AND OTHER APPLICABLE DOCUMENTATION TO THE ISSM, SO-332/GTN. REGARDING QUESTION 1, APPLICABLE DOCUMENTATION INCLUDES THE CURRENT, APPROVED DOE HQ MASTER IS SECURITY PLAN AND COPIES, SIGNED WHERE NECESSARY, OF THE FOLLOWING ATTACHMENTS:

Attachment 1 -	U/SO CODE OF CONDUCT.
Attachment 2 -	PORTABLE PERSONAL COMPUTER CONFIGURATION DESCRIPTION SUPPLEMENT.
Attachment 4 -	THIS SECURITY REVIEW CHECKLIST FOR PERSONAL COMPUTER CERTIFICATION.
Attachment 5 -	INDIVIDUAL PERSONAL COMPUTER SECURITY PLAN.

Attachment 2 IS ONLY REQUIRED FOR PORTABLE PERSONAL COMPUTERS TO DOCUMENT AND VERIFY THAT PROHIBITED FEATURES HAVE BEEN DISABLED AND REQUIRED FEATURES HAVE BEEN ENABLED. Attachment 2 MUST BE SUBMITTED WITH THE CERTIFICATION PACKAGE..